541510

8-12-05

Translation

PCT/FR2003/050202

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference SP 22237 HM	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR2003/050202	International filing date (*day/month/year*) 22 décembre 2003 (22.12.2003)	Priority date (*day/month/year*) 24 décembre 2002 (24.12.2002)
International Patent Classification (IPC) or national classification and IPC H04N 7/167, H04L 9/08		
Applicant VIACCESS		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 5 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand 20 juillet 2004 (20.07.2004)	Date of completion of this report 20 December 2004 (20.12.2004)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR2003/050202

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages 1-12, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☒ the claims:

pages _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages 1-19, filed with the letter of 26 October 2004 (26.10.2004)

☒ the drawings:

pages 1/6-6/6, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
☐ the language of publication of the international application (under Rule 48.3(b)).
☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.
☐ filed together with the international application in computer readable form.
☐ furnished subsequently to this Authority in written form.
☐ furnished subsequently to this Authority in computer readable form.
☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-19	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-19	NO
Industrial applicability (IA)	Claims	1-19	YES
	Claims		NO

2. Citations and explanations

1. Reference is made to the following documents:

D1: EP-A-0 984 630 (MINDPORT BV) 8 March 2000 (2000-03-08);

D2: US 2001/053221 A1 (TAKEDA TSUNEHARU) 20 December 2001 (2001-12-20).

2. The present application does not fulfil the requirements set forth in PCT Article 33(1) because the subject matter of **claims 1-19** does not involve an inventive step as defined in PCT Article 33(3).

2.1 Document D1, which is considered to be the closest prior art, describes (cf. in particular, column 2, lines 8-29 and the other passages cited hereinafter):

a method for securing scrambled data provided to a plurality of receiver terminals ("decrypting a message, for example, the encrypted payload in a pay TV transport stream"), each of said terminals being provided with a plurality of unscrambling modules Mj, j=1, 2 ("first and

second decryption devices") and each unscrambling module having a processing capacity and a specific security level (the first module is a smart card with "very high security" and the second is optionally a "PC or microprocessor"),

wherein

said data is pre-subdivided into a whole number of families Fj, each comprising a whole number of blocks Bi (the message is divided into blocks, some of which are transmitted to the first module, others to the second module, cf. column 2, lines 17-21 and also column 1, lines 46-51), and

each block B1 transmitted to said first module is scrambled using a key K1 ("secret key", column 2, line 13),

which method is characterised in that said blocks Bi are pre-organised based on the respective processing speeds of said unscrambling modules Mj. (The blocks in D1 are organised in such a way that the first block in a group of x blocks is transmitted to the first module, which has a slower processing speed than the second module, see, once more, column 1, lines 46-51; column 2, lines 17-21 and claim 6).

It follows that the subject matter of **claim 1** of the application differs from this known method only in that the blocks transmitted to the second module (the PC) are scrambled using a key K2 and in that keys Kj are defined on the basis of the processing capacity and the degree of security of the respective decryption modules Mj (j=1, 2).

In document D1, a more advanced algorithm is used ("error-propagating block chaining method", cf. column 2, lines 26-27) to secure said second module further and it would be very obvious for a person skilled in the art to use said method for scrambling the blocks transmitted to modules Mj in conjunction with alternative keys Kj in order to simplify the method when this additional effect is not desired. For this purpose, it would be obvious for a person skilled in the art to select keys Kj on the basis of the processing capacity and the degree of security of decryption modules Mj and thereby maximise the respective computing power of said modules.

2.2 **Independent claim 13** further differs from the known method in that it explicitly mentions an identification parameter pj assigned to each family Fj. Since the blocks transmitted to the first module in the method of D1 are not set (cf. column 1, lines 49-51: "the number of intermediate blocks is not fixed but may vary as desired"), some kind of family identification must implicitly be used.

However, this feature has already been used for the same purpose in a similar method in document D2 (see the abstract). D2 describes a method for securing scrambled data provided to a plurality of receiver terminals with a single unscrambling module. In this method, the data is also subdivided into families Fj, *explicitly* identified by means of parameters pj ("ciphering attribute") and encrypted in accordance with said parameters, which also identify the keys to be used (see page 2, paragraph [42]).

As a result, it would be obvious for a person skilled in the art to use these additional features in the method as per document D1 and thereby arrive at the subject matter of claim 13.

2.3 It would also be obvious to use said method to secure various services such as those mentioned in **claims 17-19**. It follows that said claims are not inventive either.

2.4 **Dependent claims 2-12 and 14-16** do not contain any features which, in combination with the features of any one of the claims to which they refer, might define subject matter that fulfils the PCT requirement of inventive step because all of the additional features therein are either already described in document D1 or document D2 or are unremarkable.